

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 14, 2017

Z. Li  
Huawei  
Q. Sun  
China Telecom  
Y. Zheng  
China Unicom  
March 13, 2017

**Requirements and Architecture of Carrier IP Service Models**  
**draft-li-opsawg-carrier-ip-service-model-req-arch-01**

Abstract

Service Model is a fundamental building block for a controller's North-Bound Interface (NBI). Defining a service model for different multi-layered and heterogeneous networks is a complicated work and may require lots of consideration since different model users may have different perspective and concerns.

This document proposes the requirements and architecture for service models to facilitate future work. This document does not attempt to provide a detailed description of all the architectural components, but rather it describes a set of building blocks, requirements, architecture and guidelines from which models may be constructed.

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](#)].

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 September 14, 2017.

## Copyright Notice

Copyright (c) 2017 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 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.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Terminology</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">Scope</a>	<a href="#">3</a>
<a href="#">4.</a>	<a href="#">Considerations</a>	<a href="#">6</a>
<a href="#">4.1.</a>	<a href="#">Generic Scenarios Oriented</a>	<a href="#">6</a>
<a href="#">4.2.</a>	<a href="#">Network-Functional Level Abstract</a>	<a href="#">6</a>
<a href="#">4.3.</a>	<a href="#">Multi-Level Openness Required</a>	<a href="#">6</a>
<a href="#">5.</a>	<a href="#">Requirements</a>	<a href="#">7</a>
<a href="#">5.1.</a>	<a href="#">Base Network Models</a>	<a href="#">7</a>
<a href="#">5.1.1.</a>	<a href="#">Topology Model</a>	<a href="#">7</a>
<a href="#">5.1.2.</a>	<a href="#">Inventory Model</a>	<a href="#">7</a>
<a href="#">5.1.3.</a>	<a href="#">Resource Model</a>	<a href="#">7</a>
<a href="#">5.2.</a>	<a href="#">Service Models</a>	<a href="#">7</a>
<a href="#">5.2.1.</a>	<a href="#">VPN Service Models</a>	<a href="#">8</a>
<a href="#">5.2.2.</a>	<a href="#">Service Flow Models</a>	<a href="#">9</a>
<a href="#">5.2.3.</a>	<a href="#">Tunnel Service Models</a>	<a href="#">9</a>
<a href="#">5.2.4.</a>	<a href="#">IP Flow Service Models</a>	<a href="#">9</a>
<a href="#">5.3.</a>	<a href="#">Supporting Models</a>	<a href="#">9</a>
<a href="#">5.3.1.</a>	<a href="#">QoS Profile</a>	<a href="#">9</a>
<a href="#">6.</a>	<a href="#">Architecture of Network Models</a>	<a href="#">9</a>
<a href="#">6.1.</a>	<a href="#">Principles of Architecture</a>	<a href="#">10</a>
<a href="#">6.1.1.</a>	<a href="#">Hierarchical Architecture</a>	<a href="#">10</a>
<a href="#">6.1.2.</a>	<a href="#">Extended Architecture</a>	<a href="#">10</a>
<a href="#">6.1.3.</a>	<a href="#">Three Containers</a>	<a href="#">10</a>
<a href="#">6.1.4.</a>	<a href="#">Multiple Choices</a>	<a href="#">10</a>
<a href="#">6.2.</a>	<a href="#">Architecture of Base Network Models</a>	<a href="#">11</a>
<a href="#">6.2.1.</a>	<a href="#">Topology Model</a>	<a href="#">11</a>
<a href="#">6.3.</a>	<a href="#">Inventory Model</a>	<a href="#">11</a>
<a href="#">6.4.</a>	<a href="#">Resource Model</a>	<a href="#">11</a>
<a href="#">6.5.</a>	<a href="#">Architecture of Service Models</a>	<a href="#">11</a>
<a href="#">6.5.1.</a>	<a href="#">VPN Service Models</a>	<a href="#">11</a>



<a href="#">6.5.2.</a>	Service Flow Models . . . . .	<a href="#">12</a>
<a href="#">6.5.3.</a>	Tunnel Service Models . . . . .	<a href="#">12</a>
<a href="#">6.5.4.</a>	IP Flow Models . . . . .	<a href="#">13</a>
<a href="#">7.</a>	Contributors . . . . .	<a href="#">13</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">14</a>
<a href="#">9.</a>	Security Considerations . . . . .	<a href="#">14</a>
<a href="#">10.</a>	Acknowledgements . . . . .	<a href="#">14</a>
<a href="#">11.</a>	References . . . . .	<a href="#">14</a>
<a href="#">11.1.</a>	Normative References . . . . .	<a href="#">14</a>
<a href="#">11.2.</a>	Informative References . . . . .	<a href="#">14</a>
	Authors' Addresses . . . . .	<a href="#">14</a>

## [1.](#) Introduction

Service Model is a fundamental building block for a controller's North-Bound Interface (NBI). Defining a service model for different multi-layered and heterogeneous networks is a complicated work and may require lots of consideration since different model users may have different perspective and concerns.

This document proposes the requirements and architecture for service models to facilitate future work. This document does not attempt to provide a detailed description of all the architectural components, but rather it describes a set of building blocks, requirements, architecture and guidelines from which models may be constructed.

## [2.](#) Terminology

- o NBI: North-Bound Interface
- o SBI: South-Bound Interface
- o SDN: Software-Defined Network
- o RAN: Radio Access Network
- o OAM: Operation, Administration and Maintenance

## [3.](#) Scope

The L3VPN service model [[I-D.ietf-l3sm-l3vpn-service-model](#)] is defined to provides an abstracted view of the Layer 3 IPVPN service configuration components. A typical usage is to use this model as an input for an orchestration layer who will be responsible to translate it to orchestrated configuration of network elements who will be part of the service. As the development of SDN controller, there will be functionalities division between the controller and the orchestrator. The orchestrator is always responsible for the service orchestration



between network service and related applications while controller is dedicated to the network-level services.

Since an orchestrator will face end users directly, the corresponding input for its models will absolutely be expressed into a user-friendly manner. Taking the Network L3VPN Service Model as an example, the location of PEs can be expressed by using geographical information such as street or latitude/longitude, etc. for an orchestrator model. But the input for a controller's model has to be certain identification that can be directly used by the controller such as network element ID or IP address. Though there maybe some subtle difference between the service models of controller and orchestrator, as the abstracted view of network service, there exists much similarity between these network service models. This document primarily focuses on service models for a controller's NBI instead of the counterpart of an orchestrator which are shown in the Figure 1.



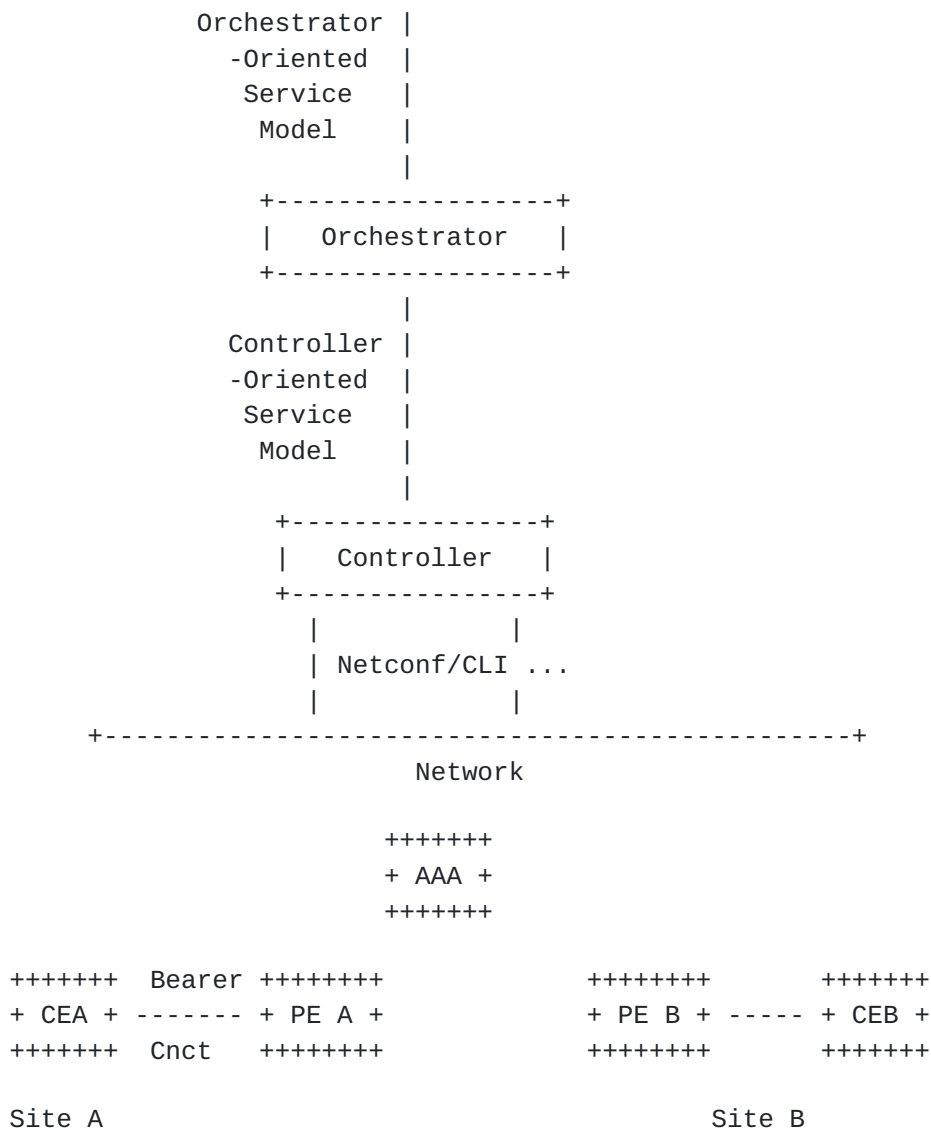


Figure 1: Different Level's Network Service Model

Currently service models such as vDC, Service Function Chain (SFC), etc. are developed for the data center network. This document focuses on the services of traditional carrier IP networks exclusively. Carrier IP networks are also facing the same challenges as those of data center networks such as rapid deployment and maintenance of network services for which network service model can be introduced to try to simplify the service provision and maintenance. For example, when handling an IP-RAN network with thousands of nodes and complex business on, it is really eager to have some methods to help to alleviate this pain point.





## **4. Considerations**

### **4.1. Generic Scenarios Oriented**

Instead of addressing all problem spaces and fixing every issue from all kinds of scenarios, a network service model is RECOMMENDED to primarily focus on those generic ones. Introducing too many details that are scenario specific can cause lots of customized models which will minimize the difference between NBI and SBI gradually and jeopardize the value of NBI in the long run.

### **4.2. Network-Functional Level Abstract**

There are two types of abstraction of network service models: Intent Level and Network-functional Level. Since the network architecture is more complicated and there will be hard to introduce many plug-and-play features, it is difficult for a carrier IP network to achieve high abstraction to the intent level. As a result, it is mandatory to understand some details of the whole network (such as service specific topology) when service models are introduced. Based on this consideration, this document will primarily focus on definition of service models of network-functional level.

### **4.3. Multi-Level Openness Required**

It is obvious that a service model can have lots of users which will certainly have different backgrounds and perspective. It is important that a service model can satisfy all these requirements through different levels of openness and abstraction while still keep itself intact.

In simple terms, we can divide the users of a service model into two groups: business users and administrators.

1. Business users. The primary concern of this kind of users is to deploy fast and operate successfully. They care about details only when they have to. Unless they are professional technical personnel or required themselves, it is better for a service model to try best to avoid unnecessary details.
2. Administrators. For administrators, they care about not only the network service provision based on the possible network service models, but also the following aspects related with network service:
  - A. Pre-configuration. In order to accomplish the mapping from NBI models to SBI models, it is necessary to pre-configure



parts of business related items and resources. This is also helpful to lower the threshold for business users.

- B. Operation and maintenance. When talking about operation and maintenance work on a daily basis, it is reasonable to access certain exact information, and even some non-user-friendly fields when shooting troubles. It is important that a service model can support such level of openness for accessing.

## **5. Requirements**

### **5.1. Base Network Models**

The base network models are to provide the abstraction of underlay network to facilitate the definition of network service models.

#### **5.1.1. Topology Model**

Topology models are the base network models to provide the abstracted view of topologies of the physical network. Based on the requirements of different network service models, there should be models on generic network topology, L3 network topology, L2 network topology, MPLS-TE topology and IP-TE topology.

#### **5.1.2. Inventory Model**

Network inventory is one important base network models which can provide the abstracted view of different network devices.

#### **5.1.3. Resource Model**

Resource model defines the configuration for pools of service resources and operational state about the used and the available resources. The model focus on the service resources such as Route Distinguisher, Route Target, Vxlan ID etc.

### **5.2. Service Models**

Nowadays huge IP related technologies such as IGP, BGP, MPLS, VPN, OAM, etc. have been used in carrier IP networks which propose the great challenges for network service provision and maintenance. When considering the procedure of deploying these services in a high abstraction level, it can be simplified as a work of "leading traffic flow into pipes". These "pipes" can be recognized as tunnels or IP flows involving multiple routers in the network, while "traffic flow" can be recognized according to different granularity. In a manner of



speaking, VPN can be seen as a kind of coarse grain flow while a finer grain flow can be defined using the "5-tuple" of IP header.

Even for the "pipes" base on tunnels, there can be many types of tunnels implemented on the device. Through a controller's NBI, an application can trigger a controller to create the tunnel it needs without understanding the detail. Or the business can trigger the traffic optimization of network-level MPLS-TE tunnels for service bearing. In these scenarios, the "pipe" itself is also a kind of network-level service. So here we get several basic service models for carrier IP network:

Pipes:

- o Network Tunnel Service Model
- o Network IP Flow Service Model

Flows:

- o Network VPN Service Model
- o Network Service Flow Model

As stated above, because of different requirements and technical background, the input of a specific service model shows the wide diversity. For instance, users of VPN Service do not have to care about it is L3VPN, L2VPN or EVPN that is actually being used. And a common end identification only needs to be designated instead of concrete IP or MAC addresses. These concrete identifications can be allocated by a controller automatically. On the other hand, some users prefer to designate the exact VPN such as L3VPN in the case IP address for the identification of ACs should be designated instead of allocated by the controller. Owing to the wide diversity of requirements on specific network service models, there should be multiple levels of such network service models to accommodate these requirements.

#### **5.2.1. VPN Service Models**

The draft "Considerations on Layered Network VPN Service Models" in process describe in details the requirements of VPN service models including:



1. Network VPN Service Model
2. Network L3VPN Service Model
3. Network L2VPN Service Model
4. P2P Network L2VPN Service Model
5. MP2MP Network L2VPN Service Model
6. Network EVPN Service Model

#### **5.2.2.    Service Flow Models**

Service flow service models is to provide the abstracted view of network-level's steering the traffic identified with the thinner granularity than VPN such as "5 tuple" of IP header to the possible "pipes". The details will be defined in the future accompanying draft.

#### **5.2.3.    Tunnel Service Models**

The draft "Considerations on Layered Network Tunnel Service Models" in process describe in details the requirements of Tunnel service models including:

1. Network Tunnel Service Model
2. Network MPLS TE Tunnel Service Model
3. Network IP Tunnel Service Model

#### **5.2.4.    IP Flow Service Models**

IP Flow service models is to provide the abstracted view of network service based on IP paths spanning multiple network elements. The details will be defined in the future accompanying draft.

### **5.3.    Supporting Models**

Supporting models is used to help define the possible service in a specific network service model. Templates or profiles of specific service are important supporting models which can be reused in the multiple instances of a specific network service models.

#### **5.3.1.    QoS Profile**

QoS Profile model can help define a set of QoS parameter which can be applied to the network VPN service models.

## **6.    Architecture of Network Models**





## **6.1. Principles of Architecture**

### **6.1.1. Hierarchical Architecture**

The architecture of network service models should be defined into a multi-level hierarchy in the object-oriented paradigm. Different concern and perspective can be fulfilled through models in different levels in the hierarchy.

### **6.1.2. Extended Architecture**

In order to adapt changes of service models, even for the network service model in the specific level of the hierarchy, there should be base model and extended model. The parameters in the base model should be common to most users while the extended model can define parameters required by limited users. If the parameters in the extended models can be well accepted, they can be moved to the corresponding base model.

### **6.1.3. Three Containers**

For specific network service models there should be three primary containers:

- Service Configuration Data: The service configuration data is used for the network service provision.
- Service Operational Data: The service operational data should be defined for operation and maintenance of the network service. There should be different levels of operational data used for business users and administrators.
- Pre-configuration. The pre-configuration can be used to define the possible policy to help convert the network service model to the device-level configuration or the service resources used for the conversion.

### **6.1.4. Multiple Choices**

There should be multiple choices for defining parameters for specific services in the network service models. For simple use cases, only few parameters need to be specified for defining a service (For example, bandwidth is specified for QoS process). But some professional users may wish to define a serial of parameters for the same service which can be achieved through a parameter template (For example, QoS profile should be introduced to define the QoS process). It is REQUIRED that options should be available for a service model to satisfy different needs.



## 6.2. Architecture of Base Network Models

### 6.2.1. Topology Model

Based on the topology models which are defining, the hierarchy of topology models are depicted in the following figure:

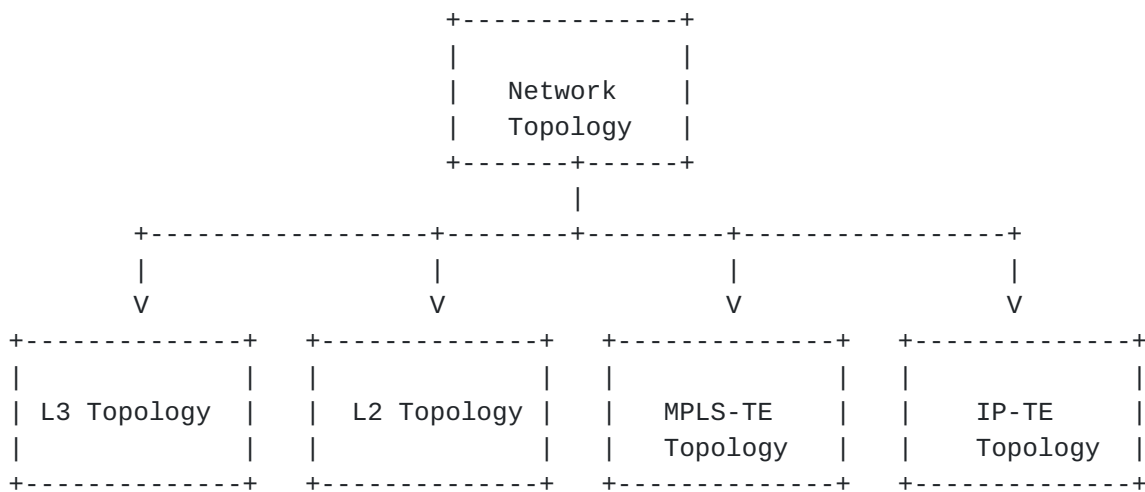


Figure 2: Architecture of Topology Models

### 6.3. Inventory Model

It will be defined in the future version of the draft.

### 6.4. Resource Model

It will be defined in the future version of the draft.

## 6.5. Architecture of Service Models

### 6.5.1. VPN Service Models

Based on the draft "Considerations on Layered Network VPN Service Models" in process, the hierarchy of VPN service models are depicted in the following figure (network EVPN model will be defined in the future version of the draft):



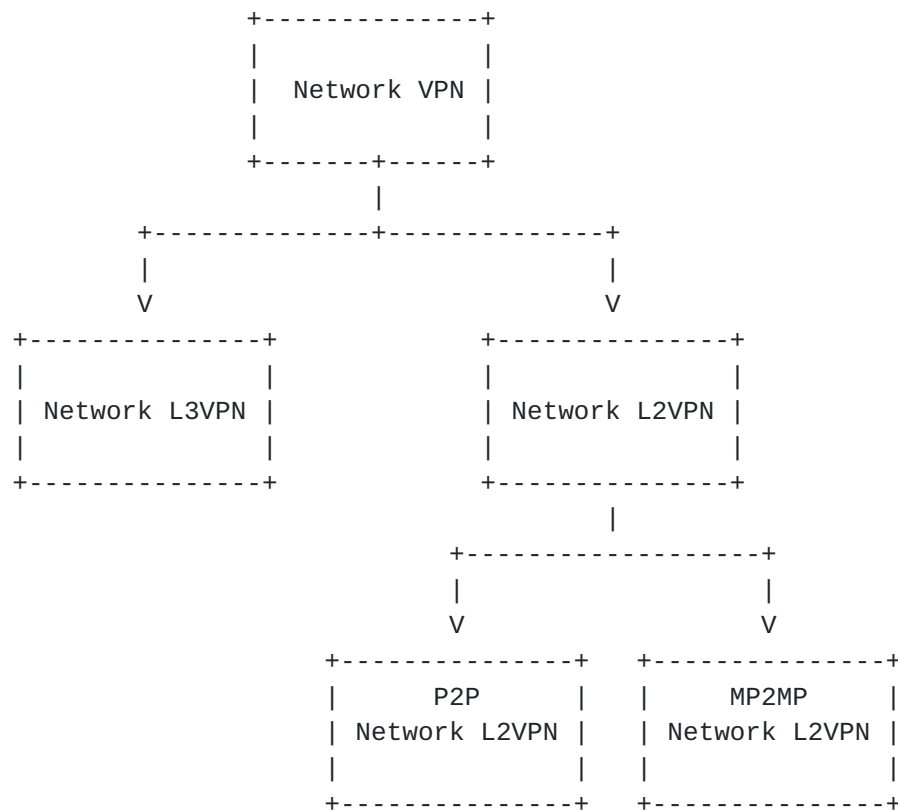


Figure 3: Architecture of VPN Service Model

### 6.5.2. Service Flow Models

The architecture of Service Flow models will be defined in the future version of the draft. Service flow service models is to provide the abstract view of network-level's steering the traffic identified with the thinner granularity than VPN such as "5 tuple" of IP header to the possible "pipes".

### 6.5.3. Tunnel Service Models

Tunnel service can be divided into TE tunnel service and IP tunnel service. The hierarchy of TE Tunnel service models are depicted in the following figure:



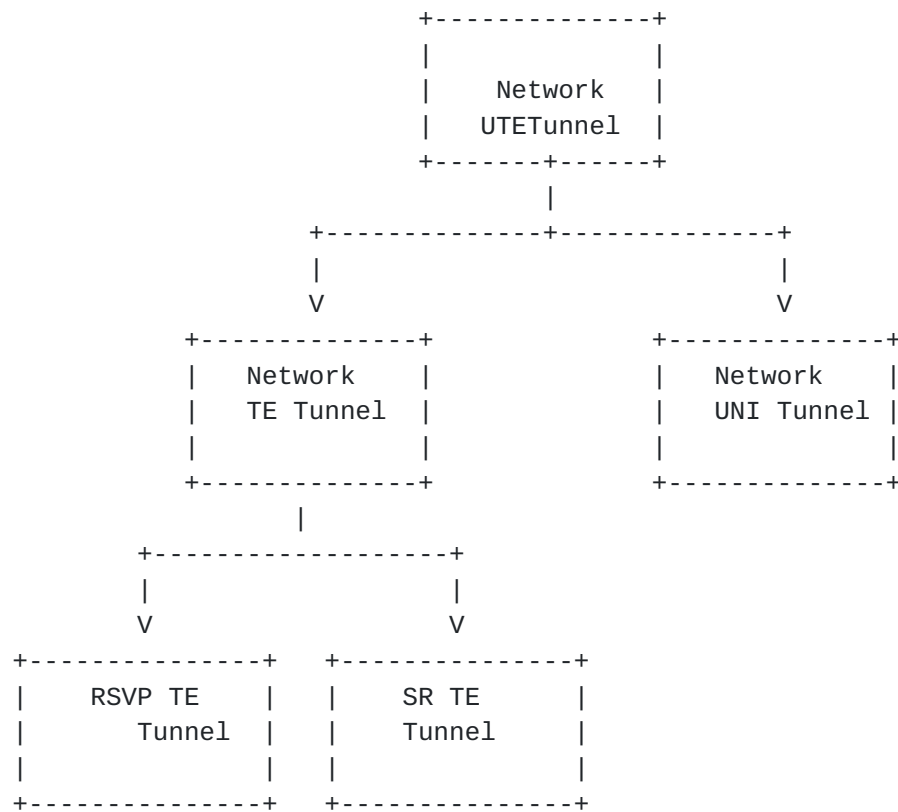


Figure 4: Architecture of Tunnel Service Model

#### 6.5.4. IP Flow Models

The architecture of IP Flow models will be defined in the future version of the draft.

## 7. Contributors

The following people have substantially contributed to the requirement and architecture design of carrier IP service models:

Xiaofeng Ji  
Huawei  
Email: jixiaofeng@huawei.com

Yuanbin Yin  
Huawei  
Email: yinyuanbin@huawei.com

Xianping Zhang  
Huawei  
Email: zhangxianping@huawei.com





## **8.    IANA Considerations**

This document makes no request for IANA.

## **9.    Security Considerations**

This document does not introduce new security threat.

## **10.   Acknowledgements**

During the course of defining requirement and architecture of carrier IP network services, the discussion with the IP experts from China Mobile, China Telecom and China Unicom does great help to this work. The discussion in the Yang models design teams of different VPNs, Tunnels, MPLS features also help much for the abstraction of network services. Research work of colleagues of authors of the draft in different controllers and orchestrators including ONOS, ODL, OpenStack, etc. provides extensive thinking on the model design. The authors would like to acknowledge all these helpful work.

## **11.   References**

### **11.1.   Normative References**

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

### **11.2.   Informative References**

[I-D.ietf-l3sm-l3vpn-service-model]  
Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN service delivery", [draft-ietf-l3sm-l3vpn-service-model-19](#) (work in progress), November 2016.

## Authors' Addresses

Zhenbin Li  
Huawei  
Huawei Bld., No.156 Beiqing Rd.  
Beijing 100095  
China

Email: [lizhenbin@huawei.com](mailto:lizhenbin@huawei.com)



Qiong Sun  
China Telecom  
No.118 Xizhimennei street, Xicheng District  
Beijing 100035  
China

Email: [sunqiong@ctbri.com.cn](mailto:sunqiong@ctbri.com.cn)

Yi Zheng  
China Unicom  
No.9, Shouti Nanlu, Haidian District  
Beijing 100048  
China

Email: [zhengyi39@chinaunicom.cn](mailto:zhengyi39@chinaunicom.cn)

