Network Working Group
Internet-Draft

Intended status: Informational
Expires: April 27, 2015

C. Zhou
T. Tsou
G. Karagiannis
Huawei Technologies
L. M. Contreras
Telefonica
Q. Sun
China Telecom
P. Yegani
Juniper Networks

October 27, 2014

The Architecture for Shared Unified Policy Automation (SUPA) draft-zhou-supa-architecture-00

Abstract

Currently, there are network services that impose specific demands on a communication network. SUPA considers two types of network services, the inter Data Center (DC) communication and Virtual Private Networks (VPN). This document describes the SUPA basic architecture, its elements and interfaces. The main SUPA architecture entities are the Network Service Agent (NSA) and the Application-based Policy Decision (ABPD). NSA is a functional entity that creates and runs network services/ ABPD is a functional entity, which 1) enables the generation, maintenance and release of i) actual/detailed network topologies and ii) VPN and inter DC service specific abstractions and 2) mapping between the VPN and inter DC service service specific abstractions and the network topology and configuration.

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 27, 2015.

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].

Table of Contents

1. Introduction

As the Internet grows, more and more new services keep on arising, and network traffic is rapidly increased, which makes network management and configuration more and more complicated, while on the other hand, dynamic and real-time configuration change is required, e.g. Inter-Data Center (DC) traffic steering and tunneling, based on real-time network status. Network applications can be used to automate the complicated and dynamic network configuration. Providing means of exposing a view of the network to applications may provide significant improvements in configuration agility, error detection and uptime for operators.

However the real value behind central configuration schemes lies within the possible simplification through abstract models provided by such systems to applications and network services running above them (on the so-called northbound side). Well-designed simplified models are able to provide a wide range of granularity for various applications and network services needs, from the lower-level

physical network to high-level application services.

An abstract view of a network infrastructure can be realized using a network graph, which describes the topology and configuration of a network. In the context of SUPA three types of network graphs are used.

The more accurate and detailed network graph type contains the details Protocol Layer 0 to Protocol Layer 7 (L0-L7) of network topology and the configuration of a network infrastructure. This is the case where resources across different layers including application layer (L7) IP/network layer (L3) and lower layers (L0-L2),e.g., MPLS, SDH, OTN, WDM) managed by the entities involved in the operations of the SUPA functional architecture. The network resources may include routers, switches, and communication links providing connectivity services for the end user application.

The second type of network graphs describes the topology and configuration of a VPN service specific abstraction, while the third type of network graphs describes the topology and configuration of a Inter-DC connectivity service specific abstraction.

The technology that can be used for this purpose is based on YANG information and data models, see [RFC6020], [RFC6991].

Network service is the composition of network functions and defined by its functional and behavioral specification. The network service contributes to the behavior of the higher layer service, which is characterized by at least performance, dependability, and security specifications.

The main goal of this document is to specify the SUPA reference architecture, its elements and interfaces.

2. Terminology

The terminology used in the SUPA problem statement draft [ID.karagiannis-supa-problem-statement] applies also to this draft.

3. SUPA Architecture

This section provides an overview of the SUPA architecture.
An overview of the SUPA architecture is given in Figure 1. The network entities used in this architecture are:

Applications: represent one or more network entities that are running and controlling network services.

Controller: represents one or more entities that are able to control the operation and management of a network infrastructure, e.g., a network topology that consists of Network Elements (NEs.)

Network Element (NE): handles incoming packets based on the network management and controlling procedures. NEs can interact with local or remote network controllers in order to exchange information, such as configuration information, policy enforcement capabilities, and network status.

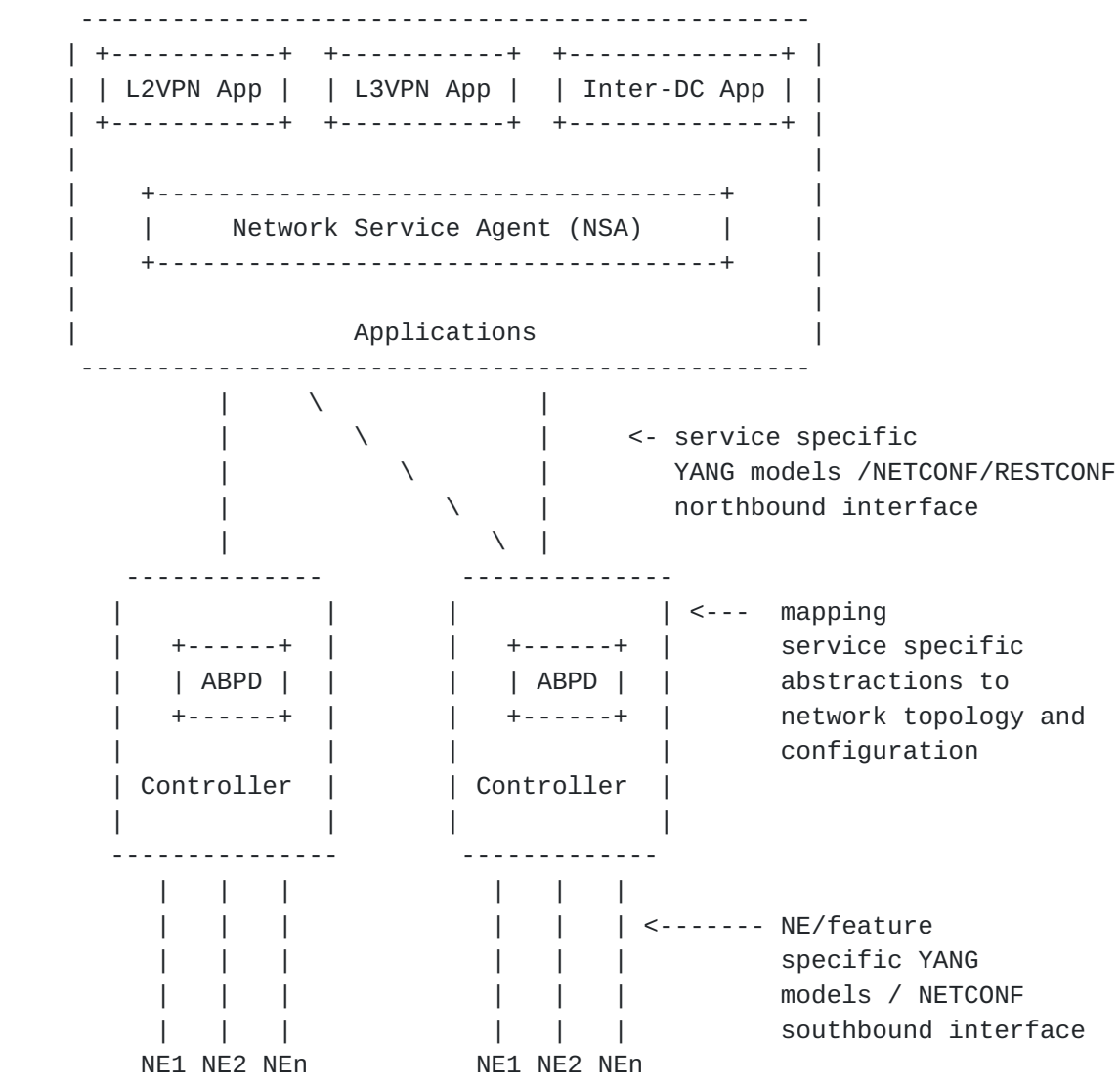

Figure 1: SUPA architecture

The SUPA architecture functional entities include the Network Service Agent (NSA) and the Application-based Policy Decision (ABPD), as shown in Figure 1. As the figure indicates support for VPN services (L2VPN & L3VPN)and Inter-DC network services are in scope for this release of the architecture. Support for other services and use cases are for further study.

Network controllers, exchange configuration information with NEs and derive the actual and detailed network topology model. When an

application needs to use this network topology it applies NETCONF [RFC6241] or RESTCONF [ID.draft-ietf-netconf-restconf] and it sends a request to receive a service specific abstraction from the network controller(s). Subsequently, the network controller(s) provides, a

service specific abstraction of the network topology to the application, which should be able to meet the requirements imposed by this application. Different types of applications may get different service specific abstractions of the same network topology from the network controller(s). For example, for the same actual network topology, a VPN network service will receive a different service specific abstraction of the network topology, than an inter-Data Center (DC) network service.

For each network service instance a service specific abstraction network graph needs to be generated and maintained. A network service can use application based demands and policies, such as tunneling or traffic steering, and possibly update its associated service specific

abstraction network graph. Moreover, by using such policies, the application can instruct the network controller(s) to map the service specific abstractions to the actual (detailed) network topology and NE specific configuration.

4. Architecture Functional Entities

In this document the SUPA architecture is expected to support two sue cases; the VPN and Inter-DC network services, see [ID.draft-cheng-supa-ddc-use-cases] for details.

4.1. Network Service Agent (NSA)

Network services can be used to provide the required configuration and application programming interfaces to support a wide variety of communication services offered by service providers.
SUPA considers two types of network services, the inter-Data Center (DC) communication and Virtual Private Networks (VPN).For each network service instance a service specific abstraction network graph needs to be generated and maintained.

The Network Service Agent (NSA) is a functional entity, residing at the Application layer, that enables network services, such as:

o) L2VPN, L3VPN, Inter-DC connectivity, and
o) request application based policies and optionally
o) update the network graphs associated with each application.

As part of the SUPA architecture operational procedures the NSA performs the following functions:

O) The NSA sends a request to the ABPD to get the service-specific information to create an abstract network graph for a given application,

o) The NSA exchanges necessary information with the ABPD regarding

any update on the network graph for a given application along with service-related policy information (e.g., tunneling or traffic-steering policy rules).

The internal structure of the NSA is depicted in Figure 2. As the figure shows the sub-functions implemented by each module includes:

o) Request Creation/Update service specific network graphs: This sub-function is used to request the information needed to create a new network graph or send an update about an existing graph. Each of the events associated with these operations are trigged via proper signaling exchange with the ABPD,

o) NSA - Network Service Interaction: this sub-function is used to provide and receive information, to/from the network service module. The main information received from the network service module is: 1) events that can trigger the request or update of a service specific network graph, or 2) application-based demands.

o) "NSA - ABPD interface": this is the interface used to support the signaling protocol exchanges between the NSA and the ABPD. Candidate protocols for such interactions are NETCONF [RFC6241] or RESTCONF [ID.draft-ietf-netconf-restconf].

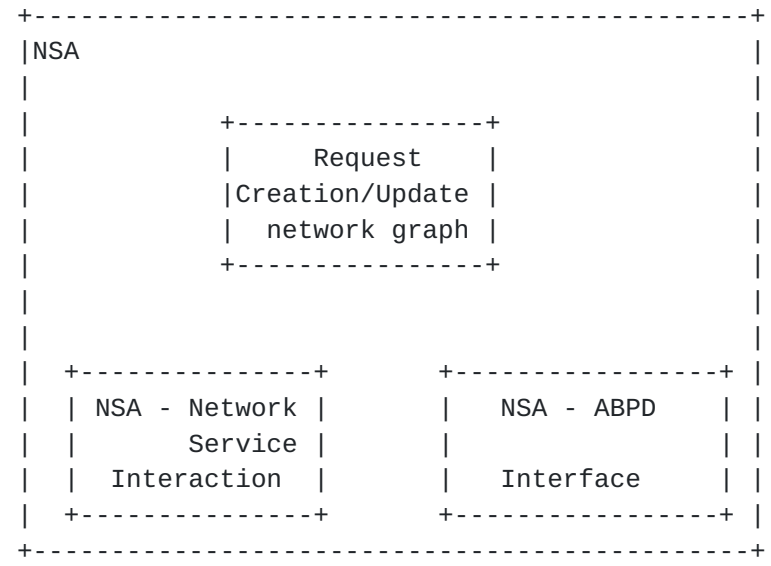

Figure 2: NSA Internal Structure

4.2. Application Based Policy Decision (ABPD)

The Application Based Policy Decision (ABPD), is a functional entity located in network controller(s) that is able to generate, maintain and release: 1) actual detailed network graph of a network infrastructure, 2) VPN and Inter-DC service-specific network graphs.

Moreover, the ABPD, supports the SUPA northbound interface/protocol. It also supports a software repository, which stores the information associated with each NE. By using application-based demands &

policies received from the NSA it can map the service-specific network graphs to the target NE and feature specific YANG models. Figure 3 illustrates the ABPD functionality block diagram, which is

based on the ABNO framework specified in [ID.farrkingel-pce-abno-architecture]. This framework was enhanced to satisfy the demands of the SUPA use cases. Note that the realization of the functional architecture defined in [ID.farrkingel-pce-abno-architecture] is out of the scope of SUPA. However, the capabilities provided by the "Provisioning manager" can be combined with capabilities provided by the SUPA defined "ABPD Network Management Interface".

The Application Based Policy Decision (ABPD) functions provides a superset of all the ABNO capabilities provided in Figure 1 of [ID.farrkingel-pce-abno-architecture]. Additional functions provided by the ABPD include:

o) Actual/detailed network service graph: maintains an up to date description of an actual/detailed network graph that models the topology and configuration of the network infrastructure controlled by the ABPD. If needed than it requests to update all databases, see Section 2.3.1.8 of [ID.farrkingel-pce-abno-architecture] for details. Moreover, it can use existing network management and signaling protocols, such as I2RS [I2RS], NETCONF [NETCONF], RESTCONF [ID.draft-ietf-netconf-restconf], etc., to request the implementation of the changes into the network status/configurations.

o) VPN service specific network service graph: maintains an up to date VPN service specific abstraction of the topology and configuration of the network infrastructure controlled by the ABPD.

o) inter-DC service-specific network graph: maintains an up to date Inter-DC service specific abstraction of the topology and configuration of the network infrastructure controlled by the ABPD.

o) Application to Network Mapping: using the application-based demands and policies received from the NSA it maps the VPN and/or Inter-DC service network graph to the actual/detailed network graph, i.e., it maps the service-specific abstractions to network topology and configuration. Moreover, this functional block provides the mapping of the actual/detailed network graph to NE/feature-specific YANG models.

o) ABPD Network Management Interface: provides the interface with existing network management, I2RS [I2RS] NETCONF, etc. protocols to request and negotiate the implementation of the changes into the network status/configuration.

o) ABPD-NSA interface: used to support the communication between the NSA and the ABPD. The candidate protocols used for this purpose could be either NETCONF [RFC6241] or RESTCONF [ID.draft-ietf-netconf-restconf].

5. Network Elements

The Network Element (NE) handles incoming packets based on the policy information communicated with the ABPD and makes corresponding policy enforcement, which is based on existing network management policies, see Section 5. An NE may be a physical entity or a virtual entity and is locally managed, whether via CLI, SNMP, or NETCONF.

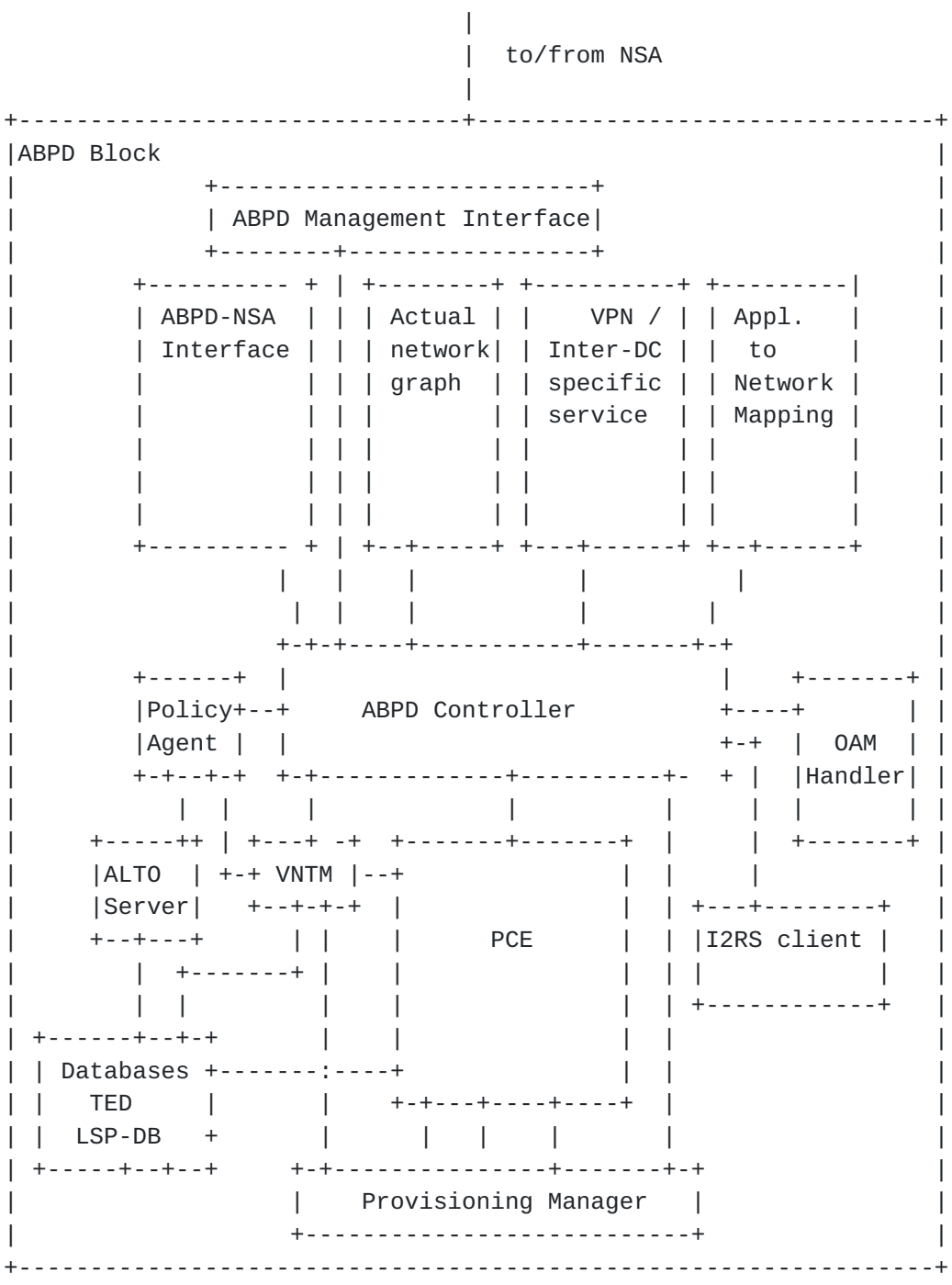

Figure 3: ABPD Internal Structure, based on
[ID.farrkingel-pce-abno-architecture].

SUPA will specify mechanisms, in order to enable the NEs to interact with either local or remote network controllers in order to exchange information, such as configuration and status information. The NEs will be able to push this information in an event or periodic basis towards the network controller or provide it after receiving a request from the network controller.

6. Security Considerations

Security is a key aspect of any protocol that allows state installation and extracting of detailed configuration states. More investigation remains to fully define the security requirements, such as authorization and authentication levels.

7. IANA Considerations

No IANA considerations.

8. Acknowledgements

The authors of this draft would like to thank the following persons for the provided valuable feedback: Diego Lopez, Jose Saldana, Spencer Dawkins, Jun Bi, Xing Li, Chongfeng Xie, Benoit Claise, Ian Farrer, Marc Blancet, Zhen Cao, Hosnieh Rafiee, Mehmet Ersue, Mohamed Boucadair, Jean Francois Tremblay, Tom Taylor.
Special thanks are expressed to the authors of the ID [ID.farrkingel-pce-abno-architecture], since a significant part of the ABPD functional blocks are based on the architecture described in [ID.farrkingel-pce-abno-architecture].

9. Normative References

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

10. Informative References

[I2RS] Interface to the Routing System (i2rs) charter, http://datatracker.ietf.org/wg/i2rs/charter/

[ID.draft-ietf-netconf-restconf] A. Bierman, M. Bjorklund, K. Watsen, R. Fernando, "RESTCONF Protocol", IETF Internet draft (work in progress), draft-ietf-netconf-restconf-03, October 2014

[ID.farrkingel-pce-abno-architecture] King, D. and A. Farrel, "A PCE-based Architecture for Application-based Network Operations", IETF Internet draft (Work in progress), October 2014.

[ID.karagiannis-supa-problem-statement] G. Karagiannis, W. Liu, T. Tsou, Q. Sun, L. M. Contreras, P. Yegani, JF Tremblay, "Problem Statement for Shared Unified Policy Automation (SUPA) " IETF Internet Draft (work in progress)", October 2014.

[ID.draft-cheng-supa-ddc-use-cases] Y. Cheng, C. Zhou, G. Karagiannis, JF. Tremblay, "Use Cases for Distributed Data Center Applicatinos in APONF", IETF Internet draft (Work in progress), draft-cheng-supa-ddc-use-cases-01, October 2014

[NETCONF] Network Configuration (netconf) charter, http://datatracker.ietf.org/wg/netconf/charter/

[RFC6020] M. Bjorklund, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC6991] J. Schoenwaelder, "Common YANG Data Types", RFC 6991, July 2013.

[RFC6241] R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

Authors' Addresses

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: cathy.zhou@huawei.com

Tina Tsou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: Tina.Tsou.Zouting@huawei.com

Georgios Karagiannis
Huawei Technologies
Hansaallee 205,
40549 Dusseldorf,
Germany
Email: Georgios.Karagiannis@huawei.com

Luis M. Contreras
Telefonica I+D
Ronda de la Comunicacion, Sur-3 building, 3rd floor
Madrid 28050
Spain
Email: luismiguel.contrerasmurillo@telefonica.com
URI: http://people.tid.es/LuisM.Contreras/

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

Email: sunqiong@ctbri.com.cn

Parviz Yegani
JUNIPER NETWORKS
1133 Innovation Way
Sunnyvale, CA 94089
Email: pyegani@juniper.net