

Network Working Group
Internet-Draft

Intended status: Informational
Expires: November 08, 2015

C. Zhou
Huawei Technologies
L. M. Contreras
Telefonica
Q. Sun
China Telecom
P. Yegani
Juniper Networks
May 08, 2015

The Framework of Simplified Use of Policy Abstractions (SUPA)
draft-zhou-supa-framework-02

Abstract

Currently, there are network services that impose specific demands on a communication network. This document describes the SUPA basic architecture, its elements and interfaces. The main SUPA architecture entities are the Service Management (SM) and the Network Manager/Controller (NM/NC). The SM is a functional entity that creates and runs network services by using a set of NM/NCs. The NM/NC is a functional entity that provides one or more of the following functions: (1) the generation, maintenance and release of network topologies, (2) the generation, maintenance, and release of network service-specific abstractions, (3) the mapping between network service-specific abstractions and the network topology, and (4) the mapping between network service-specific abstractions and network device configuration. Both the SM and the NM/NC may be made up of multiple distinct entities that collectively perform their functions.

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.

Copyright Notice

Copyright (c) 2014 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.

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.

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 Content

| | |
|--|---|
| 1. INTRODUCTION | 2 |
| 2. TERMINOLOGY | 3 |
| 3. SUPA FRAMEWORK | 4 |
| 4. FRAMEWORK FUNCTIONAL ENTITIES | 6 |
| 4.1. SERVICE MANAGEMENT | 6 |
| 4.2. NETWORK MANAGER/CONTROLLER | 6 |
| 4.3. NETWORK ELEMENTS | 7 |
| 5. SECURITY CONSIDERATIONS | 8 |
| 6. IANA CONSIDERATIONS | 8 |
| 7. ACKNOWLEDGEMENTS | 8 |
| 8. NORMATIVE REFERENCES | 8 |
| 9. INFORMATIVE REFERENCES | 8 |
| AUTHORS' ADDRESSES | 9 |

1. Introduction

As the Internet grows, new services are created, new devices are connected, and new users use the Internet. These and other factors contribute to the significant increase in the amount and type of network traffic. This in turn makes network management and configuration more and more complicated.

However, the need for dynamic and real-time configuration changes is required. One example is Inter-Data Center (DC) traffic steering and tunneling, based on real-time network status. Dedicated network management applications are required to automate the complicated and

dynamic network configuration present in today's systems. Such applications need interoperable data models of network topology, network services, and policy rules to support the design, deployment, and maintenance of network services. Providing these data models to network management applications may provide significant improvements in configuration agility, error detection, and uptime for operators.

However, in order to scale and to ensure configuration change consistency, existing network configuration schemes must be simplified through the use of abstraction. This increases the programmatic control over such systems. 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 one or more network topology data models. Each such topology model, whether physical or logical, may be used as its own reusable managed object. This enables existing topologies to be reused to create new topologies. This applies to models of different layers, including the application layer (L7), IP/network layer (L3), and lower layers (L0-L2, such as MPLS, SDH, OTN, WDM). The network resources may include physical and/or virtual network nodes and links.

A network service data model is service specific, and usually relies on a network topology data model. The network service data model defines the behavior of the network service, which is characterized by one or more metrics that include performance, dependability, and security specifications.

One method to automate service configuration is to use a policy data model. Policy, in conjunction with network service and device data models, can be used to tell the Network Manager/Controller (NM/NC) how to generate Network Element (NE) configurations using network service data models in combination with topology data models. For example, this process can be used to choose a path for VPN which will involve a set of NE's.

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

YANG data models (e.g., see [RFC6020], [RFC6991]) can be used for representing service and topology models.

2. Terminology

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

| | |
|----|--------------------|
| NE | Network Element |
| NC | Network Controller |
| NM | Network Manager |

NM/NC Network Manager/Controller
 SM Service Management

3. SUPA Framework

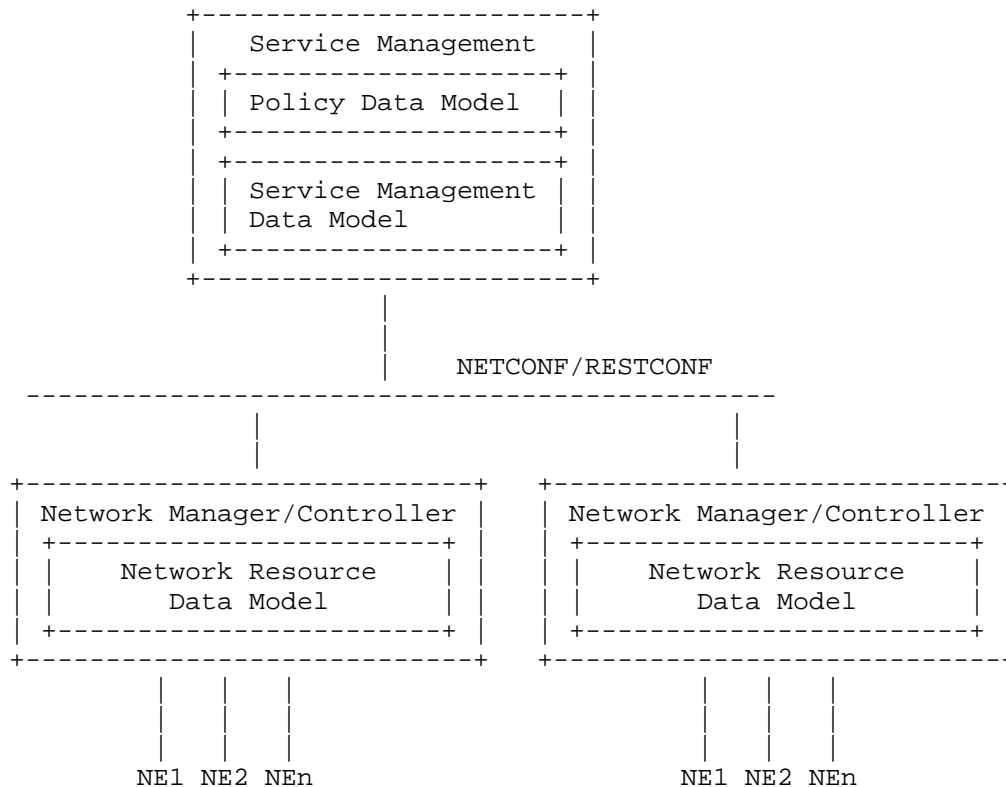


Figure 1 SUPA Framework

An overview of the SUPA framework is shown in Figure 1. The network entities used in this framework are:

SM: Service Management, which represents one or more network entities that are running and controlling network services.

Policy Data Model

Model of policy rules for managing the network service and mapping services dynamically to the network topology and network resources. Policy data models are used to describe high level service requirements, such as routing requirements.

Example of policy data model can be found in [ID.draft-strassner-supa-generic-policy-info-model] and [ID.draft-bi-supa-policy-model].

There can be various types of policies, including service specific policies and network-wide policies. There can be a

centralized entity managing the network-wide policies, which may be called as policy manager. The policy manager can be located in the SM or in a separate location.

Policy data models now considered by SUPA are generic policy data model, ECA (event, condition, action) as described in SUPA charter. The work may be extended in the future.

Service Management Data Model

Model of the network service (e.g., VPNs) and the network resources required by the network service to be correctly deployed and executed on the physical and/or virtual topology.

Example of service management data model can be found in [ID.draft-zaalouk-supa-vpn-service-management-model].

NM/NC: Network Manager / Controller, which 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 Resource Data Model

Model of the physical and virtual network topology including the resource attributes (e.g., data rate or latency of links) and operational parameters needed to support service deployment over the network topology.

Example of network resource data model can be found in [ID.draft-contreras-supa-yang-network-topo]

SUPA will not define network resource data model, which is out of the scope of SUPA. SUPA will make use of network resource data models defined by other WGs or SDOs.

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

Service Management (SM) communicates with Network Manager/Controller (NM/NC) using an appropriate protocol, such as NETCONF [RFC6241] or RESTCONF [ID.draft-ietf-netconf-restconf].

NM/NC exchanges configuration information with NEs and derives the current network topology that contains the NEs, and also the capabilities and status of NEs, which will be stored in network resource data model. NM/NC may also communicate with traditional network management system to retrieve the above information. It can use existing network management and signaling protocols, such as I2RS [I2RS], NETCONF [NETCONF], RESTCONF [ID.draft-ietf-netconf-restconf], etc.

Service Management (SM) will send policy data model and service management data model, which will in conjunction with network resource data model be mapped to detail NEs' configurations by network manager / controller.

4. Framework Functional Entities

4.1. Service Management

There are a wide variety of communication services offered by service providers.

The Service Management (SM) is a functional entity, residing at the Application layer, which enables network services, such as:

- o) Network services (e.g., L2VPN, L3VPN, etc.)
- o) application-specific policies

SM will push service management data model and policy data model to NM/NC for service deployment.

4.2. Network Manager/Controller

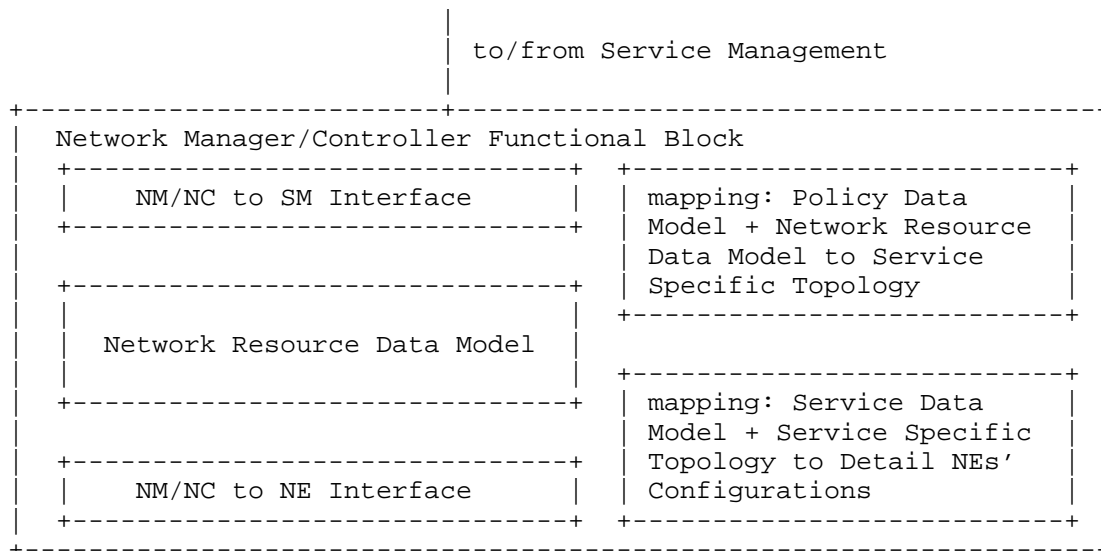


Figure 2 NM/NC Functional Blocks

Network Manager/Controller (NM/NC) is a functional entity that is able to generate and maintain desired and current topologies of the network infrastructure. As part of this process, it is also responsible for reserving and releasing network resources that are required to support network services in a given network infrastructure.

The NM/NC contains a set of data models, functions and APIs, including:

- o) Network Resource Data Model
Maintain an up to date topology of the network infrastructure, including capabilities and current status of NEs.
- o) Mapping: service specific topology
This mapping procedure will combine the policy data model and service management data model and generate a specific topology.
- o) Mapping: target NE(s) detail configurations
This mapping procedure will use the service specific topology generated in the previous procedure and the service management data model to generate detail NE(s) configurations.
- o) NM/NC to traditional network management system interface:
provides the interface with existing network management system protocols (e.g., I2RS [I2RS], NETCONF, etc.) to request configuration and status information, and push configuration changes to NEs.
- o) NM/NC to SM interface: used to support the communication between the SM and NM/NC. The candidate protocols used for this purpose could be either NETCONF [RFC6241] or RESTCONF [ID.draft-ietf-netconf-restconf].

An example of the mapping procedures can be that, a service requires that a link from A to B is created; and the policy requires that the hops of this link should not exceed N. Then when NM/NC receives the policy data model and service management data model from SM, it will first apply the policy data model to the network resource data model and get a sub-set topology which can fulfill the hops limit requirements. Then NM/NC will further generate detail configurations for target NE(s). The mapping procedures can be enforced by functional entity called policy agent.

After the service is deployed, if there is a network topology change, network configurations for this service may need to be updated accordingly. A possible solution is to repeat the mapping procedures, and generate configurations for NEs (maybe another set of NEs). This requires that NM/NC maintains a copy of the service management data models and policy data models.

For more detail about mapping mechanisms, please refer to [ID.draft-pentikousis-supa-mapping].

4.3. Network Elements

The Network Element (NE) responds to requests and commands from the NM/NC and makes corresponding configuration changes. An NE may be a physical or a virtual entity, and is locally managed (e.g., via CLI, SNMP, or NETCONF).

SUPA will specify mechanisms, in order to enable the NEs to interact with either local or remote network management systems. The

interaction may include the exchange of information, such as configuration and status information. The NEs will be able to push this information in an event that the NM/NC can subscribe to, and/or provide this information after receiving a request from the NM/NC.

5. 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.

6. IANA Considerations

No IANA considerations.

7. 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, Tina Tsou, Georgios Karagiannis, John Strassner, Raghav Rao, Jing Huang.

Early version of this draft can be found here:

<https://tools.ietf.org/html/draft-zhou-supa-architecture-00>

At the early stage of SUPA, we think quite some issues are left open, it is not so suitable to call this draft as "architecture". We would like to rename it to "framework". Later there may be a dedicated architecture document.

8. Normative References

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

9. 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-04, January 2015

[ID.karagiannis-supa-problem-statement] G. Karagiannis, Q. Sun, L. M. Contreras, P. Yegani, JF Tremblay, " Problem Statement for Simplified Use of Policy Abstractions (SUPA)" IETF Internet Draft (work in progress)", draft-karagiannis-supa-problem-statement-06, March 2015.

[ID.draft-cheng-supa-ddc-use-cases] Y. Cheng, JF. Tremblay, J. Bi, L. M. Contreras, "Use Case for Distributed Data Center in SUPA", IETF Internet draft (Work in progress), draft-cheng-supa-ddc-use-cases-06, April 2015

[ID. draft-zaalouk-supa-vpn-service-management-model] D. Zhang, A. Zaalouk, K. Pentikousis, Y. Cheng, "VPN Service Management YANG Data Model", IETF Internet draft (Work in progress), draft-zaalouk-supa-vpn-service-management-model-03, April 2015

[ID.draft-strassner-supa-generic-policy-info-model] J. Strassner, "Generic Policy Model for Simplified Use of Policy Abstractions (SUPA)", IETF Internet draft (Work in progress), April, 2015

[ID.draft-bi-supa-policy-model] J. Bi, R. Tadepalli, M. Hayashi, "DDC Service Policy YANG Data Model", IETF Internet draft (Work in progress), March, 2015

[ID.draft-pentikousis-supa-mapping] K. Pentikousis, D. Zhang, "Simplified Use of Policy Abstractions (SUPA): Configuration and Policy Mapping", IETF Internet draft (Work in progress), draft-pentikousis-supa-mapping-04, March 2015

[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

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