Network working group
Internet Draft
Category: Standard Track

Vic Liu
China Mobile
L. Xia
Huawei
Zu Qiang
Ericsson

Expires: December, 2014

June 30, 2014

# Network as a Service Architecture
# draft-liu-nvo3-naas-arch-01

Abstract

This draft provides an high-level overview architecture of Network as a Service (NaaS) system, and describes how every component of it works together from different aspects (i.e., data plane, control plane, management plane, etc) of NaaS system.

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/1id-abstracts.txt.

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

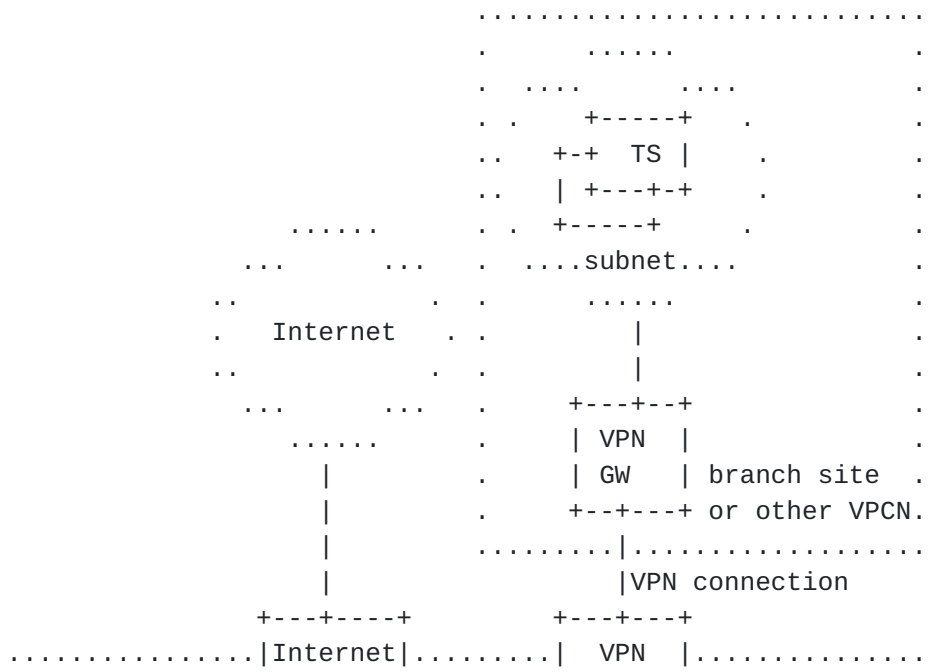
This Internet-Draft will expire on December 30, 2014.

Table of Contents

## 1. Introduction

Network as a Service (NaaS) is a new network business model provided by more and more operators. It is a novel class of services for cloud computing that provides virtualized E2E connectivity to end users at different levels of reliability, traffic QoS and transparency in a flexible and scalable way. From the technical point of view, the essential part of it is network virtualization. That means, virtual network (including sub-network, gateway, network routing, bandwidth, network service, etc) as the resource provided by operator, can be got on-demand by clients by the way of pay as you go service. Clients can make the network provision and use their own virtual network flexibly according to specific requirements. By this way, operators' network infrastructure can be virtualized and multiplexed for selling, and clients can improve the flexibility of their network to reduce cost because of better visibility and efficient control over their own virtual network.

The common use case for NaaS is to construct the virtual private cloud network (VPCN) for tenant (i.e., enterprise, organization, etc) over the public cloud provided by operator. Its main characteristic is that tenant can custom their own VPCN, i.e., network topology, VPN connection, network services, etc. Following Figure 1 is an example for VPCN:



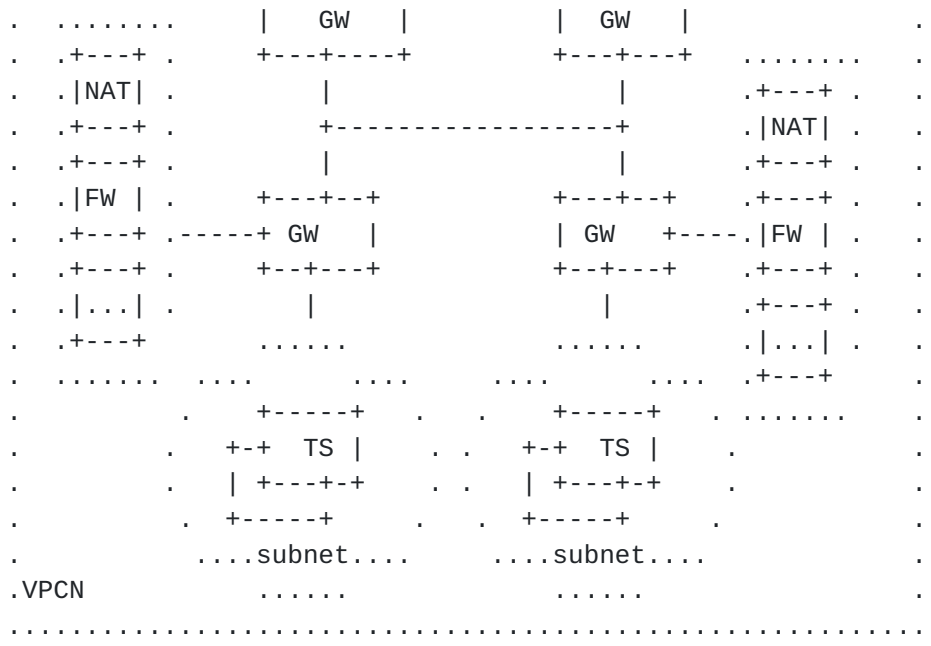



Figure 1: VPCN example

In a VPCN, tenant has several subnets for different application or service, gateways work for the inter-subnet traffics. Some network services (i.e., NAT, FW, etc) may be needed to work together with gateways. If the VPCN provides services to internet, or needs to access to internet, the internet gateway is needed to support this. The VPCN can also have the VPN gateway for interconnecting tenant's branch sites or other VPCNs through VPN connections.

In addition to the VPCN, a complete NaaS system consists of other components. They involve different aspects of NaaS system, i.e., data plane, control plane, management plane. This draft provides an high-level overview architecture of NaaS system, and describes how every component of it works together from different aspects of NaaS system.

## 1.1. Conventions used in this document

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].

## 1.2. Terminology

To be added.

## 2. Overview

For better understanding what influence NaaS may introduce into current network technologies, this section gives a brief summary of new features and main challenges introduced by NaaS.

### 2.1. New Features

NaaS introduces a lot of new features to current network for consideration; most of them are listed below:

- Network virtualization: NaaS must support Multi-tenancy requirement. And it should hide the implementation details of the network infrastructure;

- Close integration with virtual IT resources (compute, storage): NaaS must have the capabilities of VM auto-discovery, integrated operation/provision together with IT resources;

- Elasticity/High Availability: NaaS must have the capabilities of on-demand bandwidth allocation, dynamic link/network creation, dynamic and geographically distributed pools of shared ICT resources, etc;

- Flexible service chain: Flexible interposition of various middle boxes in the NaaS network becomes an essential and valuable requirement for it and an IETF WG (SFC: Service Function Chaining) has been created to study and resolve the series of requirements;

- SDN paradigm: SDN is optional paradigm, but provides great flexibility and efficiency in network resource management, optimized path selection for DC interconnection;

- Automation: This feature should be achieved in many aspects for saving manual labor, which includes automatic collection of the network topology information, policy auto distribution, OAM, auto recovery, etc;

- Open interface to user: Making virtual network resource can be managed by user themselves. For simplifying the operation, this interface should provide network resource abstraction/presentation, comprehensive service template, etc.

### 2.2. Main Challenges

Despite the above features introduced by NaaS, a series of challenges also appear in front of the implementation, as listed below:

- Constraints of physical DC: Traditional network technologies such as vlan, broadcast domain, acl, firewall setting, etc, have put so much constraints because of their location dependent feature;

- Distributed subnet: One L3 subnet can span across the whole DC by virtualization technology. Hosts in a L3 subnet are no longer limited in one location. This kind of distributed subnet scenario brings new challenges of hosts' unified identification and access control;

- Programmable network: SDN paradigm needs to define information model and data model used by the related interfaces, and the information mapping between overlay and underlay network;

- On-demand and flexible service chain: It means dynamic service awareness and automatic service provision;

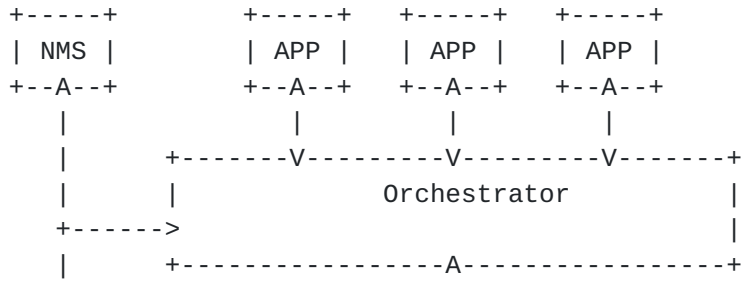
- End to end connection provision: How to provide the End to end VPN service to users when the wan/man network and DC network are separated? How to integrate enterprise's current infrastructure and NaaS in cloud seamlessly and securely? How to guarantee the End to end SLA, including bandwidth, latency, etc?

- Backwards compatibility and smooth migration;

- Security related issue;

## 3. NaaS Architecture

A complete and high-level architecture of NaaS system is shown in Figure 2 followed:



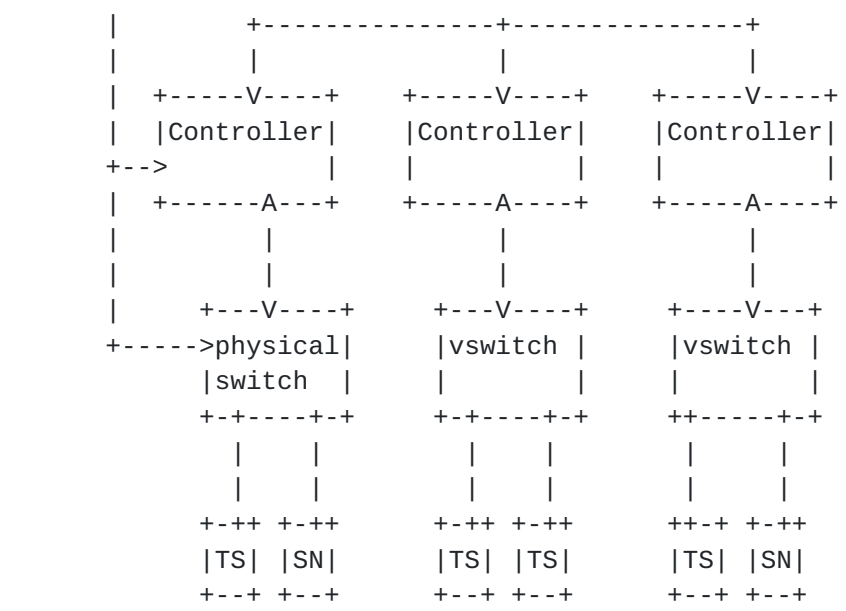



Figure 2: NaaS Architecture

In the above architecture, a NaaS system can divide into 4 layers:

- Application layer This layer consists of application (APP) and/or network management system (NMS). Applications having the visibility to network resource is beneficial for them to use network resource better. Various standard interfaces can be used among applications and orchestrator, i.e., Restful API, Java, JSON, netconf, etc. NMS is used for the management or configuration of the network devices (i.e., physical/virtual switch), policies in controller, etc. NMS is an independent system which can communicate and manage objects of every layers;

- Orchestrator layer: This layer is mainly used for integrating all the resource (i.e., computing, store, network, etc) and controlling them in centralized way. By providing standard interface in northbound and southbound, it can support different types of controller and hide the difference from application layer;

- o Controller layer: The core layer for the NaaS system. It is responsible for transforming service requests from application layer into forwarding information (e.g., flow table) in the network devices. It collects network states, status and warnings from network devices and synthesizes them for the path computation. It can distribute various policies (i.e., ACL, QoS, access control, etc) to network devices. Controller can be the centralized or distributed system. It uses standard protocols (i.e., Openflow, Netconf, I2RS [I-D.ietf-i2rs-architecture], BGP-LS [I-D.ietf-idr-ls-distribution], etc) to communicate with network devices;

- o Network layer: This layer consists of all the network devices for switching traffic, also all the tenant systems (TS) and service nodes (SN: i.e., FW, NAT, etc). The network devices and service nodes receive the forwarding information and policies from controller layer and process the traffic in data plane accordingly.

Four layers of component work together through standard interfaces and protocols among them, form a complete and high-level architecture of NaaS system.

In the following sections, NaaS system is described in details from different aspects.

## 4. Data Plane of NaaS System

In data plane, NaaS system is mainly related to the network layer. Depending on the network scalability and traffic throughput of it, the provision of network layer can have two models: centralized NaaS network and distributed NaaS network.

### 4.1. Centralized NaaS Network

Main characteristic of centralized NaaS network is the centralized gateway and related service nodes normally located at the core or aggregation layer of network. This deployment model is more suitable for small/middle scale network. Most tenant systems are in the layer 2 network, traffic among them is switched locally. Other types of traffic (i.e., inter network traffic, internet traffic, VPN traffic, etc) among a small part of tenant systems need to traverse the centralized gateway and related services nodes to get the unified process.

### 4.2. Distributed NaaS Network

Being opposite to centralized NaaS network, distributed NaaS network requires multiple gateways and related service nodes can be distributed in different places of network. This helps to improve the overall network performance and avoid the single point of failure. This deployment model is more suitable for large scale network. Most of the inter network traffic is processed locally in the distributed gateway and related service nodes.

### 4.3. Comparison

To be added.

## 5. Control Plane of NaaS Network

To be added.

## 6. Management Plane of NaaS Network

To be added.

## 7. Security Considerations

TBD.

## 8. Acknowledgements

## 9. IANA Considerations

The document does not require any IANA action.

## 10. References

### 10.1. Normative References

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

### 10.2. Informative References

[I-D.ietf-i2rs-architecture] Atlas, A., Halpern, J., Hares, S., Ward, D., and T.Nadeau, "An Architecture for the Interface to the Routing System", (work in progress), February 2014

[I-D.ietf-idr-ls-distribution] Gredler, H., Medved, J., Previdi, S., Farrel, A., and S.Ray, "North-Bound Distribution of Link-State and TE Information using BGP", (work in progress), November 2013.

Authors' Addresses

Vic Liu
China Mobile
32 Xuanwumen West Ave, Beijing, China
Email: liuzhiheng@chinamobile.com

Liang Xia
Huawei Technologies

Email: frank.xialiang@huawei.com

Zu Qiang
Ericsson
8400, boul. Decarie
Ville Mont-Royal, QC,
Canada

Email: Zu.Qiang@Ericsson.com