TBD
Internet-Draft
Intended status: Informational
Expires: May 14, 2015

Y. Lee
Comcast
R. Ghai
Benu Networks
November 10, 2014

Problem Statements of Virtual Home Network
draft-lee-vhs-ps-02

Abstract

Network Virtualization is proven a success to more effectively manage services in data center. This draft states the motivations and problem statements of decoupling services from Customer Premises Equipment (CPE) and virtualizing them in the Network Service Provider (NSP).

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 May 14, 2015.

Table of Contents

1. Home CPE

In the early days of Internet era, most users used dial-up directly connecting to Internet from desktop Personal Computer (PC). Network Service Provider (NSP) offered a single public IPv4 address to the dial-up (i.e., PPP) connection to the PC. This model was revised when Internet and PC became more popular. Multiple PCs would share a single NSP connection. NSP wanted to preserve the model to offer only a single public IPv4 address per connection, NAT [RFC2663] enabled Customer Premises Equipment (CPE) was introduced in home network. When days advance, NSP are offering more and more IP services (e.g., video, voice, home automation), NSPs must provide seamless support and excellent services to their users. Today CPEs are doing more than just NAT-ing. They may include but not limited to the following services:

- IPv4 NAT Services
- DHCPv4 Server Service
- Personal Firewall Services
- Parental Control Service
- Voice over IP (VoIP) Service
- Home Monitor Service

- Video Streaming Service

- DNS Proxy Service

2. CPE Deployment Model

Although the current CPE deployment model is a by-product of limited public IPv4 addresses, it is proven a successful model to serve users. More importantly, in the past NSP network had limited service capacity in the network and the capacity wasn't growing as fast as the user demand. NSP could offload and distribute their services to the CPE so that NSP can focus on growing bandwidth capacity. With all the CPE's successes, there are also some drawbacks:

- No Uniform set of Services: There is no uniform set of services. CPE vendors can't build an one-for-all-NSP CPE. Each NSP may offer slightly different set of services; hence, each NSP may develop its CPE specifications for CPE vendors to build.

- Service Variation: Even for a well defined service, each NSP may still have different requirements. For example: NSP-A may use SIP for its VoIP and NSP-B may use WebRTC.

- CPE Manageability: When an NSP plan to offer a new service that is not compatible to the current CPE. The NSP must update or upgrade the CPE. Depending on the NSP subscription base, it could mean to update or upgrade thousands to millions of CPEs.

Among all three, CPE manageability is particularly critical to NSP.

3. Customizable Service

The revolution of portable smart device and Internet-of-Thing has radically changed the service definition for NSP. In the past, only personal computers were connected to the Internet. NSP service model was to provide the best connectivity to a household. Household members didn't usually carry multiple devices and didn't streaming HD videos to different type of devices, so the service model was providing best Internet connectivity for the entire household. Fast forward to today, portable smart devices are personalized. A typical user may carry 2 to 3 devices that are constantly connected to Internet. Besides, many electronic devices such as sensors, monitoring systems, appliances and entertainment systems are all connected to the Internet. These devices may have different service requirements. Some may have strict latency requirement (e.g. webcam and online gaming) and others may have strict bandwidth requirement (e.g. high-definition video streaming). These new requirements cause the NSP to rethink a pure connectivity service model to a

customizable service model. This requires the NSP to build a network that could identify packet flows and associated them to user profiles and apply proper policies to them.

Since the IPv4 addresses are depleted, IPv6 emigration has finally started. One major advantage of IPv6 is network transparency. In IPv4, NSP and Content Service Provider (CSP) can't identify a device simply by examining just an IPv4 address because a public IPv4 may represent multiple devices behind NAT. In IPv6, every device will have one or more Global Unicast IPv6 addresses (GUA). This enables NSP and CSP to offer device and user specific services. This inspires innovation in new end-to-end services. For NSP, they may refine and evolve the current "heavy" CPE deployment model to speed up offering new services.

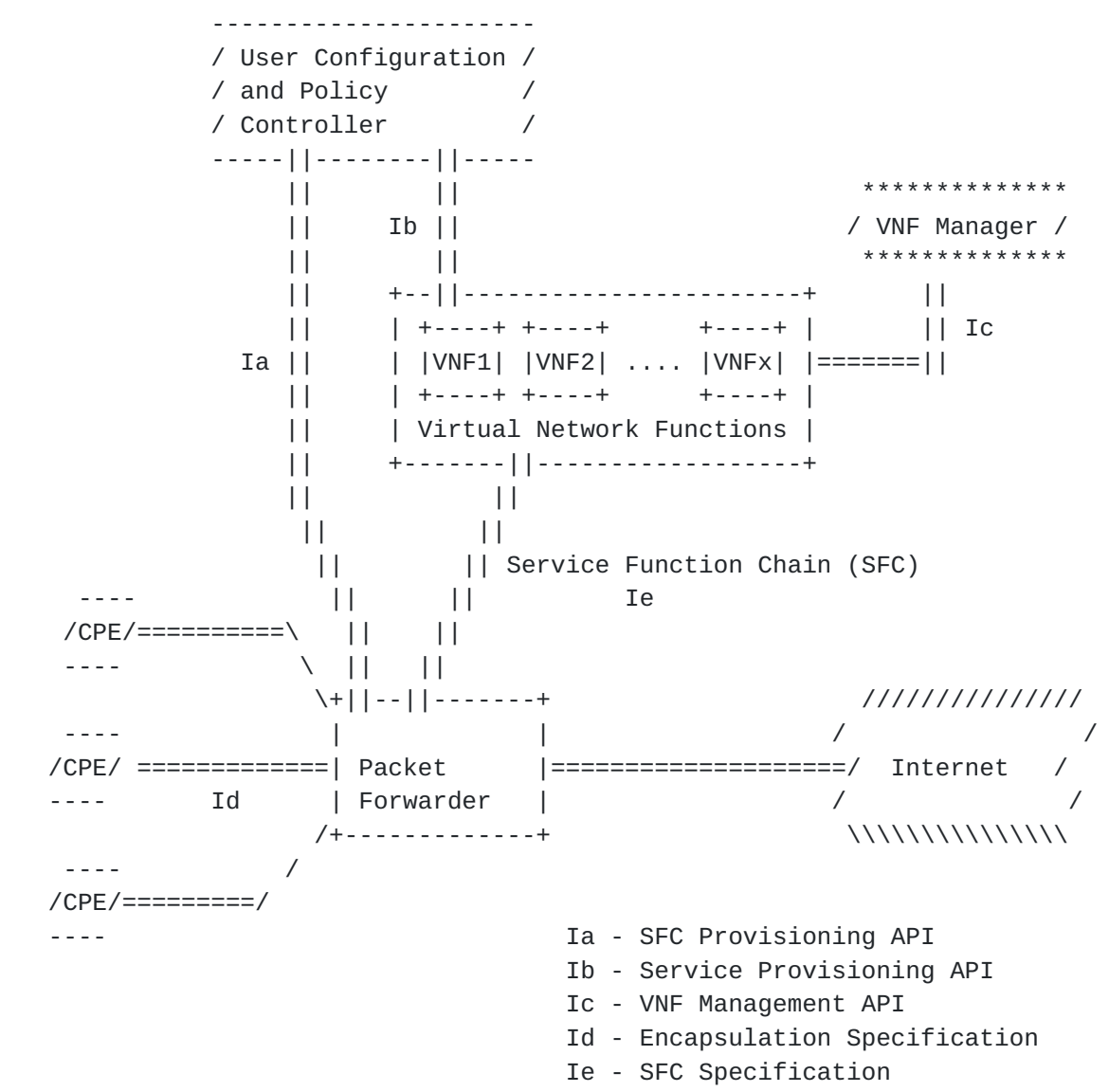
4. Network Virtualization

Software Defined Network (SDN) is originally designed to decouple network software functions from hardware. Service designers can focus on service development without coupling to the underneath hardware architecture. SDN provides a set of Application Programming Interface (API) for service designers to interact with the hardware for packet processing. There are two critical criterion to make this concept possible: Fast network and Exponential growth of computation power in general purposed hardware. Recently many NSPs have agreed that these two criterion are met with current technology.

Network Function Virtualization (NFV) aims to define a framework to allow typical network functions such as NAT, firewall and QoS policy management running on Virtual Machine (VM). NFV can combine with SDN and convert the traditional hardware centric networking architecture to more software centric networking architecture. Many NSPs are seriously considering to apply the SDN and NFV concept to re-architect the core and edge network design.

5. High-level Architecture

Similar to classic SDN architecture, Virtual Home Network (VHN) includes a Controller (VHNC) that contains user configurations and policies and a Packet Processor (VHNF) that process packet forwarding. Similar to class NFV architecture, VHN includes a set of Virtual Network Functions (VNF) and a VNF Manager (VNFM) managing the VNF. Figure 1 shows the high-level VHN architecture.



Virtualizing Home Services High-Level Architecture Diagram

Figure 1

In Figure 1, it shows five interfaces. Ia, Ib and Ic are interfaces for control protocols. Id and Ie are data path specifications.

- Ia between the VHNC and the VHNF is used to exchange configuration and policy. For example: User A's living room TV has Committed Information Rate (CIR) set at 10Mb/s and must be protected by firewall function implemented in VNF.

- Ib between the VHNC and VNFs is used to exchange configuration and policy For example: VHNC could configure the firewall VHF to block any incoming ICMP messages to the User A's living room TV.

- Ic between VNFM and VNFs is used to exchange VHN management messages. For example: VNFM could instantiate a new firewall VNF when the current firewall VNF reached certain capacity.

- Id is the protocol agreed between CPE and VHNF. It could be Ethernet or any encapsulation technology such as PMIP or MPLS.

- Ie is the Service Chaining Function protocol between VHNF and VNF. SFC WG is currently defining the specifications.

VNF contains the service definitions and service logic. For example: Virtual Network Function 1 (VNF1) could be a parental control service and manage web filter rules configured by subscriber. Virtual Network Function 2 (VNF2) could be personal firewall that protects a home from botnet and intrusion. NSP can scale VNFs horizontally to meet user demand. NSP can also dynamically create VNF per subscriber only when the subscriber wants that service. For example: NSP initiates VNF1 for User X and VNF2 for User Y. In this model, NSP no longer updates CPE for service addition or modification.

VHNC stores the user's service subscription. Each user may have different set of home services. For example: User A may have video service. User B may have VoIP service. VHNC contains the user's service subscription and interact with the VNF modules to provide proper services to users.

VHNF is usually a networking device that is optimized for processing packet. It is also implemented the Service Function Chain function to forward user packets to proper VNFs.

CPE is a simple access device that connects to the subscriber's devices at home to the NSP network.

6. Problem Statement

Virtual Home Network enables NSP to offer service in a more rapid pace. It also enables NSP to offer new possible services such as:

1. Connect a user mobile device to his home network at outdoor access point.

2. Provide more flexibility IPv4 and IPv6 address management.

3. Provide more granular QoS management.

Section 5 describes the high-level architecture. One possible deployment is to put the VHNC in a central location and put the VHNF closer to users. This deployment requires to standardize the following:

- Service Definition: Define the service semantics and user interaction. This allows the vendor community to standardize the service definition and build the Virtual Service model to support it.

- Ia: Define and specify the API to provision the user configuration parameters to the VHNF and Service Function Chain.

- Ib: Define and specify the API to provision service parameters to VNFs.

- Id: Define new header format to carry user id and device id in the packet.

Standardizing the Service Definitions, Ia and Ib will simplify service integration and equipment interoperability. This will help vendors to speed up development and NSP to speed up new service offering.

7. Security Considerations

8. Conclusion

9. Acknowledgements

10. IANA Considerations

This memo includes no request to IANA.

11. References

11.1. Normative References

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

11.2. Informative References

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

Authors' Addresses

Yiu L. Lee
Comcast
One Comcast Center
Philadelphia, PA 19103
U.S.A.

Email: yiu_lee@cable.comcast.com
URI: http://www.comcast.com

Rajat Ghai
Benu Networks
300 Concord Road, Suite 110
Billerica, MA 01821
U.S.A.

Email: rghai@benunets.com
URI: http://www.benunets.com