VNF BOF
Internet-Draft
Intended status: Informational
Expires: July 25, 2014

S. Hares
K. Subramaniam
ADARA

January 21, 2014

Use Cases for Resource Pools with Virtual Network Functions (VNFs)
draft-hares-vnf-pool-use-case-00

Abstract

In the context of virtualization, a service essentially consists of a set of Virtualized Network Functions (VNFs) with each VNF building on top of virtualization infrastructure to implement a specific network functions along with the data connections between VNFs. VNFs may be highly distributed existing in devices in data center networks, mobile networks or satellite networks. In some of these environments, the resources are highly constrained.

This draft provides seven use cases the authors have implemented in demonstration or deployed code for the following network function virtualization: cloud bursting, parental controls, load balancer for multipath (L1-L7), WAN optimization that runs either between access nodes and Data Centers, WAN optimization between mobile phones to Data Centers (through access nodes), application placement optimization, and optimized placement of web applications utilizing minimal data transfer.

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 July 25, 2014.

Table of Contents

1. Introduction

There is a trend to virtualize certain network services within the access networks, data center networks, and WAN networks. This service virtualization has been considered as part of the network function virtualization or the Software Defined Networking (SDN) technology development. This draft focuses on the implementation of these network services using units of virtual network function (VNF) denoted as a VNF set where the each VNF implemented as a pool of VNF instances. Each VNF build its VNF instances on top of virtualization infrastructure to implement a specific network function (NF) connected to other network functions (NFs). For example, a VNF Firewall will have a pool of virtual firewall instances. When VNF instances are highly distributed (such as in a DC network or some

access edge nodes for IP RAN) virtual function instances are built on resource constraint environment where resource contention, hardware status change, hardware or software failure may encounter.

This introduction introduces the terms, lists deployed VNF use cases documented in this draft, and summarizes the problems that Virtual Network Function Pools have.

1.1. Terms

The VNF Problem statement [I-D.zong-vnfpool-problem-statement] defines the terms reliability, VNF, VNF Pool, VNF Pool Element, VNF Pool User, VNF Pool Manager, and VNF Set. This draft uses these defintions. The following definitions are not defined within the VNF problem statement: Cloud Bursting, stateful parental controls, WAN optimization, and application placement. These terms are defined below.

Cloud Bursting: is the ability for Virtual processing to burst through the limits of one virtual environment and automatically transfers a portion of the processing to another virtual environment.

Stateful parental controls: is the ability for network access devices to have content filters that react to traffic, location, and user. These controls follow the user across multiple access points within a home network, or in a carrier network.

WAN optimization: is the ability to optimize traffic across a Wide-Area network. WAN optimization often makes use of TCP FLOW optimizations (with IETF TCP features) and TCP de-duplication of packets,

Application placement: is ability for coordinating software to place applications based a combination of compute resources, data storage, network service, and security concerns. Application placement may involve movement of some application data, movement of some applications (data and compute), and movement of network resources to service the applications. One type of network resource movement is the movement of virtual network functions (VNFs) which are defined, created, allocated with resources in a way to provide an integral unit to the application placement control software.

OTT (Over the Top): This industry terms implies an overlay network that is overlaid on existing networks as a virtual network.

1.2. Use Case List

The use cases described in this draft are:

- Cloud Bursting
- stateful parental controls implemented in access nodes and firewalls (stateful and regular)
- load balancer doing multipath (supports L1-L7 optimization),
- WAN optimization between access nodes and Data Centers,
- WAN optimization between mobile phones through access nodes to/ from Data centers,
- Application placement optimization using optimized DNS and DCHP VNFs,
- Application placement optimization utilizing minimized data transfer.

These use cases are based on our experience with deployed product. To make the Network Functions deployable and interoperable, these use cases should be considered in the design of the functions. These use cases are described in term that align with the VNF Pool Problem statement.

Deployment of multi-vendor interoperability VNF services requires protocols and interfaces to VNF Pools that VNF Managers can access. Enterprises and Carriers have indicated their desire to allow the multi-vendor promise of SDN to be realized in the VNF functions.

1.3. VNF Problems

VNF in constrained environments encounter the following types of problems: shared risk during VNF failures, VNF instance transition, backup and state synchronization of VNF within VNF sets, appropriate placement of VNF, reliable transport, and and multi-tenancy issues.

(Note: The VNF Problem statement [I-D.zong-vnfpool-problem-statement] has not included multi-tenancy issues.

Shared risk group

Shared risk groups occur when different VNF instances are built on top of the same instance of a virtualized platform (E.g. hypervisor). When a hypervisor fails, all the VNF instances will on the same

hypervisor will fail, and service chains with this hypervisor VNFs in the remote chain will fail. Several concurrent services will fail when a hypervisor fails. If a fail and a restart occur quickly, it may placed substantial load on the network as effective VFN chains cause other nodes to be impacted.

A VNF instance may encounter varying conditions on available resources during hypervisor load, resource contention from other NFV or application programs running. The resources may be unavailable due contention with other programs placing load on the hypervisor, or hardware failures, software failure, or DOS.

VNF instance transition

If the VNF is unable to get the appropriate resources, the VNF meta-controller/manager may decide to migrate the function to another hypervisor or another portion of the network. Appropriate resources may include CPU resources, storage resources, special hardware resources, memory, and network resources. Another reason for varying conditions of resources is the need to add additional VNF to provide the appropriate level processing. For example, if additional in-depth analysis of a data pattern in a traffic flow was determine further security actions, another VNF set with DPI inspection and analysis might be created.

Backup and state synchronization

Backup systems are needed for any system requiring high reliability or high availability. Virtualized network services desired by customers may include network services critical to security of a network, user service levels, or insuring continued network availability during network outages. Planned network outages require transition of virtualized network services to other portions of the network. Transitions during planned outages have two cycle (transition before outage, transition after outage).

Other than VNF transition, VNF instance will fail due to either hardware or software failure in various levels such as hypervisor, VM or even program. During a software failure, the VNF functions or group of functions may expand to synchronize state, handoff processes, and announce backup. This state synchronization may be limited to one hypervisor or spread across several hypervisors.

Multi-tenancy

When different users cohabitate the same VNFs or different VNF cohabitate the same hypervisors, cohabitation may cause conflicts. Just as different human roommates sharing a common kitchen

facilities, may have different traffic patterns so do different users utilizing the common VNFs. To stretch the metaphor, suppose one roommate wants to clean cooking pot immediately after use while the second roommate wants to wash cooking pots at the end of his/her cooking preparation. At some point, the roommates might content for the sink to wash dishes. In the same way, data flows wanting to share a Deep packet inspection (DPI) engine may find that cohabitation in the multi-tenant DPI may cause issues. Different levels of reliability will also impact how multiple tenants share their resources. Resource pools allow both VNFs to get the common resource when desired by virtualizing it.

2. Cloud Bursting Use Case

Description:

Three cases of cloud bursting exist. Public cloud adding more resources upon demand. Private cloud adding more resources upon demand from private cloud resources. Private cloud adding more resources from the public cloud. In the public/private cloud, the orchestration system looks within pools of additional resources to fit the request for more resources for a particular time. ADARA has demonstrated these features in public forums (ONS 2012, ONS 2013) in products shown in a cloud bursting in joint demo with Verizon (2012) operating over open-source hypervisors (2012, 2013). Commercial products with this code have been deployed in large networks.

Behind each function is a set of resource pools with VMs that do a specific function (NFV or processing) and ability to configure vswitch, vrouting, and vtransport (TCP/STCP) via libvirt, CLI, REST, and JASON. The following is a list of functions that the cloud bursting retains pools for:

- Virtual Machines (VMs) for application processing
- VMs for remote storage drops
- NFVs for firewall
- NFVsfor DDOS
- NFVs for specialized DNS/DCHP after private/public cloud move
- VMs for movement of data and applicatinos within Cloud (Private/ Public) or between clouds
- VMs for VPN to user

Why VNF Pools: Bursty nature of action of Cloud Bursting requires being able to pre-allocate pools of VNF instances prior to use. Multi-vendor interoperable VNF Pools allows Data Center operators in Enterprise and Carriers to avoid the single-source for purchasing and single-code source software-bug failures.

3. Stateful Parental Controls

Description:

Parental content filters are targeted filters that are installed based on an identification of a user. When the SDN meta-controller detects the User (via program use, user-id on program, or traffic/ port match), the SDN installs the appropriate software to guarantee filters. Two types of security exist: authentication and authorization. In authentication, ACL and other port based filtering is set per customer for the user. This filtering may block, prioritize, or transfer to a blackhole recording device different traffic. In authorization, the systems create a web of trust via an identity server (for HTTP 1.0 SAML template defined by OASIS and IETF ABFAB information for non-http).

These stateful content filtering functions were demonstrated at at ONS 2012/2013 by ADARA for Verizon network (ONS 2012), and for open source hypervisors, switches, and routers (juniper/cisco). More sophisticated policy based on bandwidth, delay, n-tuple is deployed in commercial environments.

The following is a list of some of the VNFs associated with this that utilize our pool facility:

- VNF(s) for open source DPIs (snort, etc)
- VNFs for specialized DPI inspection
- VNFs for probes on hypervisors"
- VNFs for depositing configuration in SDN OFS switches, and non-SDN switches, routers, firewalls, access nodes
- VNF(s) for firewall
- VNFs for DDOS
- VNFs for specialized DNS/DHCP services after private/public cloud move
- VNFs for movement within Cloud (Private/Public) or between clouds

- o VNF(s) for VPN to user identification

Why VNF Pools: Bursty nature of user access that is data dependent requires being able to pre-allocate pools of services prior to use. Multi-vendor interoperable VNF Pools Enterprise and Carriers to avoid the single-source access devices for purchasing and single-code source software-bug failures in access nodes.

4. Load balancer

Description:

Load balancers look to balance traffic different layers of the stack (L1-L7). ADARA's SDN meta controllers monitor work with the time-critical OTT control process (which creates and manages the OTT VPNs (L2/L3/MPLS)) to determine where the load is at any specific time, and to track it over time. The SDN orchestrators work with the SDN OTT control process to adjust to readjust the load at L1-L7.

The VNF functions that use resource pools in the load balancing service are:

- o VNFs for probes in all devices (mobile phone, ipad, access devices, vswitch, vrouter, tcp optimizer, DPI, hypervisors, VMs dumming storage, VMs creating the network;

- o VNFs for depositing configuration in SDN OFS switches, and non-SDN switches, routers, firewalls, access nodes;

- o VNFs for firewall;

- o VNFs for Traffic capacity/load balance calculation;

- o VNFs running orchestrator monitor/change algorithms;

- o VNFs for traffic movement within Cloud (Private/Public) or between clouds to balance load; and

- o VNFs for VPN to user identification.

Why VNF Pools: True end-to-end Load balancing requires a load balancing across multiple layers. with VNF pools to support different functions. Multi-vendors solutions will allow meta controllers to balance traffic to reduce costs in networks. Current Enterprise customers find the load balancing operates with TCP WAN optimization to utilize all network bandwidth effectively.

5. Android phone TCP WAN optimization

Description:

Android phones and Android pads often communicate across the LTE/WiFi connections. Optimization of the link for the low-bandwidth of LTE or Wifi connections, and the switch between LTE and WiFi requires monitoring of traffic, choosing link, optimizing TCP (Window and removing duplicates).

The VNFs that use resource pools in this application include:

- VNFs for probes in all devices (mobile phone, mobile pads, Wifi enabled nodes, LTE IP RAN notes)
- VNFs for depositing configuration in SDN access nodes (Wifi or LTE)
- VNFs for to handle remote phone parameter adjustments;
- VNFs to do firewalls (E.g traffic not allowed over LTE due to customer policy);
- VNFs for TCP data de-duplication process;
- VNFs for Traffic capacity/load balance calculation (see Football stadium problem below);
- VNFs for best processing of Video traffic or best network to pull Video traffic from;
- VNFs for VMs for VPN to user identification; and
- VNFs to interface to secure data processes.

One scenario to consider is the football stadium scenario. A person takes the IPAD to watch the close up replays or send email. During fourth quarter, the person receive an urgent call to go home and walks with the IPAD down the street to the metro-system to return home. On the way, the person is utilizing the IPAD to send mail, watch the football game, and do Skype calls.

Why VNF Pools: Phones systems do not want a single vendor for all features. Multiple interoperable access nodes and Android pad/tablet implementations require these VNF pools.

6. SOHO device optimization

Description:

SOHO devices using SDN VM technology must balance traffic movement between small cells (WiFi or femtocells). Access policies must be configured for restriction on this policy.

The VNFs that use resource pools in this application are:

- VNFs for probes in all devices (mobile phone, mobile pads, WiFi enabled nodes, LTE or femtocells)
- VNFs for depositing configuration in SDN access nodes (Wifi, L), VNFs for handling remote phone parameter adjustments;
- vNFs for firewall (traffic not allowed over LTE);
- VNFs for TCP data de-duplication process;
- VNFs for Traffic capacity/load balancing over single/multiple soho links;
- VNFs to allow applications load balance across internal soho links based on traffic needs and use policy; and
- VNFs for VPN to user identification and security.

Why VNF Pools: SOHO devices often need to be plug and play for different types of users. Common VNF Pools allows development of interoperable devices that can plug and play under a SOHO controller.

7. application scaling

Description:

Applications may be placed in a variety of hypervisors. The rapid deployment of applications on services may allow millions of applications to be available within the cloud. Creating a effective lookup for the applications or redirecting applications takes an Network Virtual environment that controls DCHP, DNS, and http access rapidly. 2 Million URI references for each access node is possible given the current growth.

VNF within the cloud must scale up to handle the VNF services required by the network infrastructure. This includes the network information functions of DNS, DCHP, URL processing, AAA (Diameter/

Radius). Fast enactment of these network functions allows an on-demand creation of a multi-tennancy overlay (IETF NV03).

The VNFs that use resource pools in this application are:

- VNFs for AAA functions (Diameter, Radius);
- VNFs for DNS functions;
- VNFs for DCHP functions
- VNFs for specialized URL/URI processing;
- VNFs for handling remote probes on these virtual information functions;
- VNFs for handling remote configuration of these virtual information functions;
- VNFs for Traffic capacity/load balance calculation;
- VNFs for determine optimium deployment of full VMs for application or determination if data transfer to an existing application (Java Application data);
- VNFs for VPN to user identification and permissions to use data; and
- VNFs to determine back-up placements for applications

8. IANA Considerations

This document includes no request to IANA.

9. Security Considerations

This document has no security issues as just contains use cases.

10. References

10.1. Normative References

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

10.2. Informative References

[I-D.zong-vnfpool-problem-statement]
Zong, N., Dunbar, L., and M. Shore, "Problem Statement for Reliable Virtualized Network Function (VNF)", draft-zong-vnfpool-problem-statement-01 (work in progress), September 2013.

Authors' Addresses

Susan Hares
ADARA
7453 Hickory Hill
Saline, CA 48176
USA

Email: shares@ndzh.com

Karthikeyan Subramaniam
ADARA
First Street
San Jose, CA
USA

Email: ksubramaniam.adarnetworks.com